RENU

Security Awareness Lab

By Daniel Kawuma <dkawuma@renu.ac.ug>

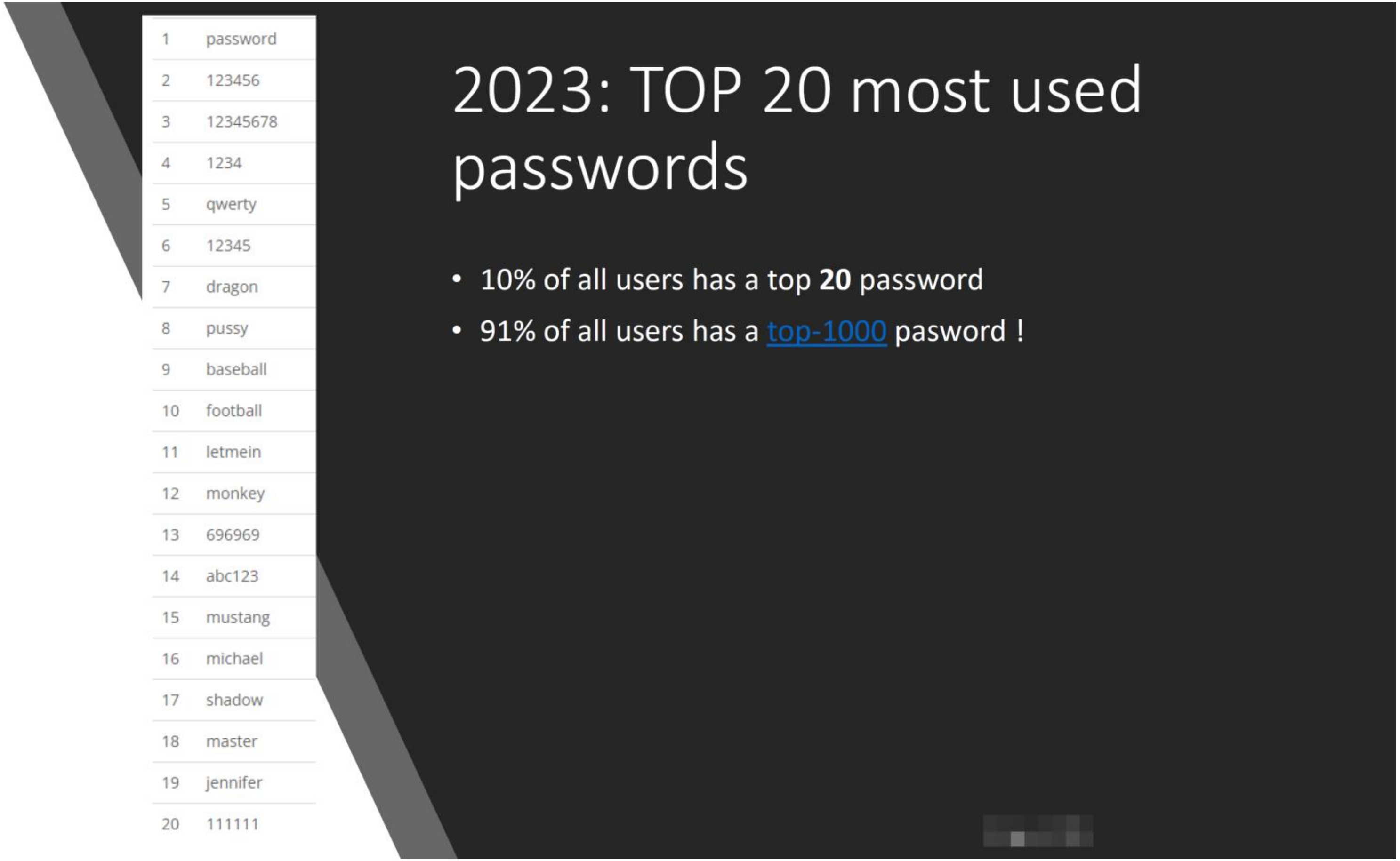
RENU

Security Awareness Labs

Enabling Research & Education Collaboration

Outline

- Passwords
- Browsers and extensions
- Data/Password Breaches
- OSINT
- Tips and Advice



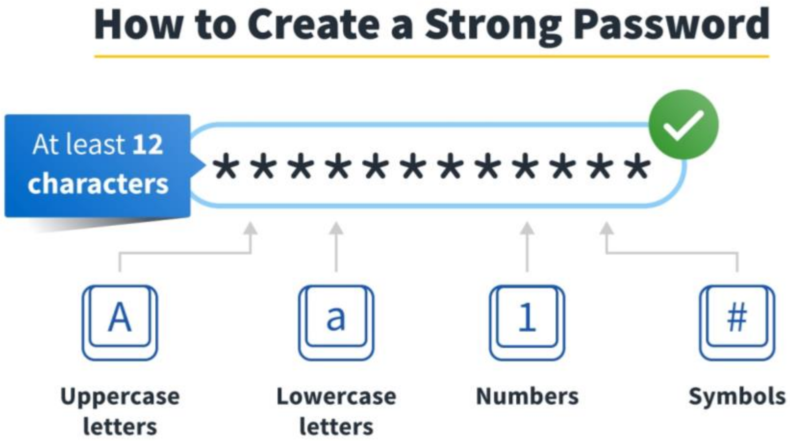
1	password
2	123456
3	12345678
4	1234
5	qwerty
6	12345
7	dragon
8	pussy
9	baseball
10	football
11	letmein
12	monkey
13	696969
14	abc123
15	mustang
16	michael
17	shadow
18	master
19	jennifer
20	111111

2023: TOP 20 most used passwords

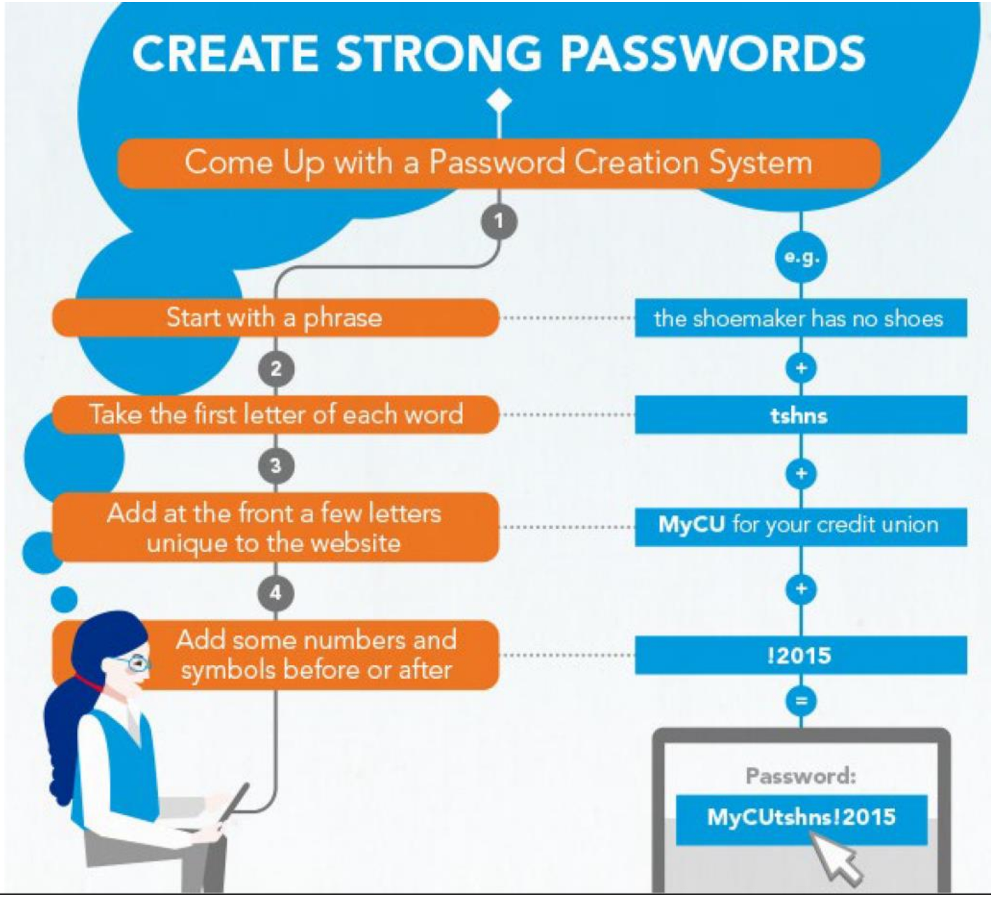
- 10% of all users has a top **20** password
- 91% of all users has a top-1000 pasword !

Strong Password Tips…

- One password per service/website
  - Never re-use a password
- Don't use "password reminder sentences"
  - Or better lie!!!
- Use Password managers
- At least 12 characters



How to remember a strong password?



CREATE STRONG PASSWORDS

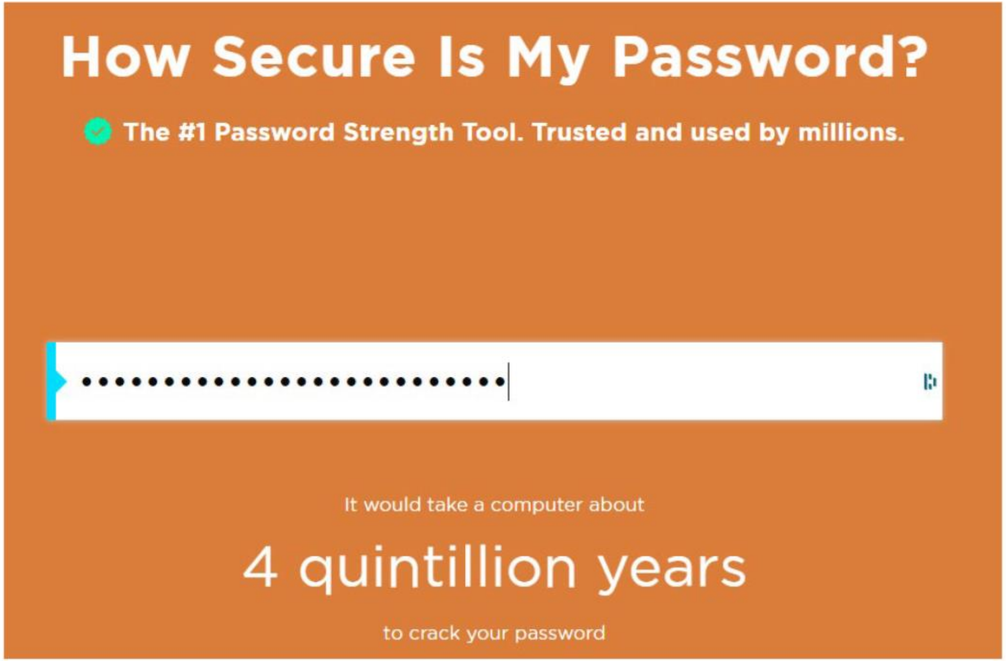
Come Up with a Password Creation System

1. Start with a phrase — e.g. the shoemaker has no shoes
2. Take the first letter of each word — + tshns
3. Add at the front a few letters unique to the website — + MyCU for your credit union
4. Add some numbers and symbols before or after — + !2015

= Password: MyCUtshns!2015

The ultimate password?!

- https://www.security.org/how-secure-is-my-password/



How Secure Is My Password?

✓ The #1 Password Strength Tool. Trusted and used by millions.

•••••••••••••••••••••••••••

It would take a computer about

4 quintillion years

to crack your password

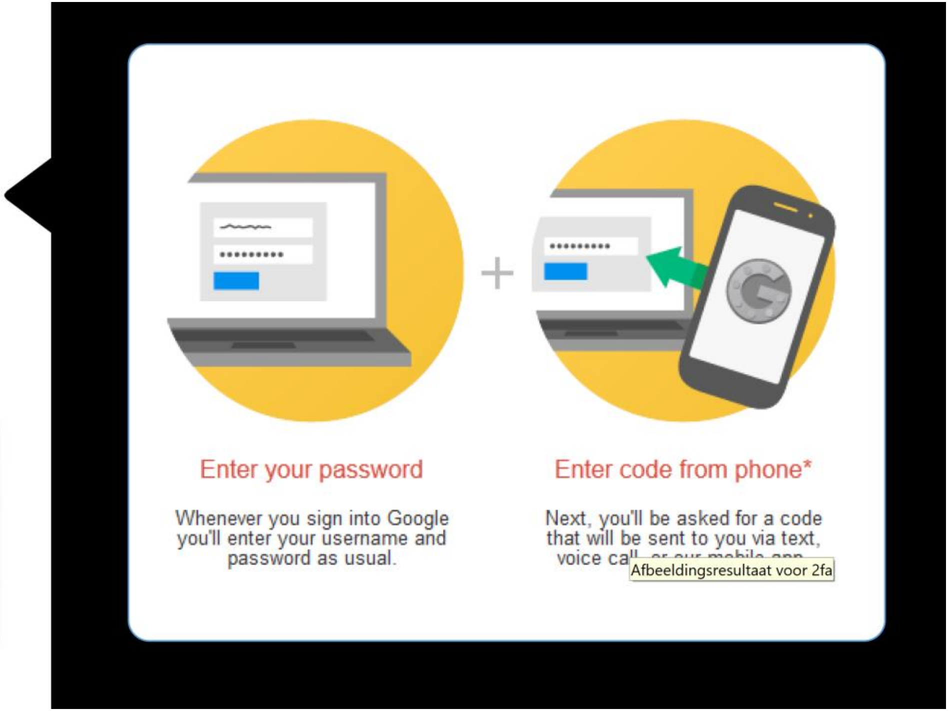
Get (any of) **these** password managers **NOW**!!!

AND their browser extensions

Use 2FA

- 2-factor authentication: use your phone (eg sms) as additional security

SOMETHING YOU KNOW
+
SOMETHING YOU HAVE



Enter your password

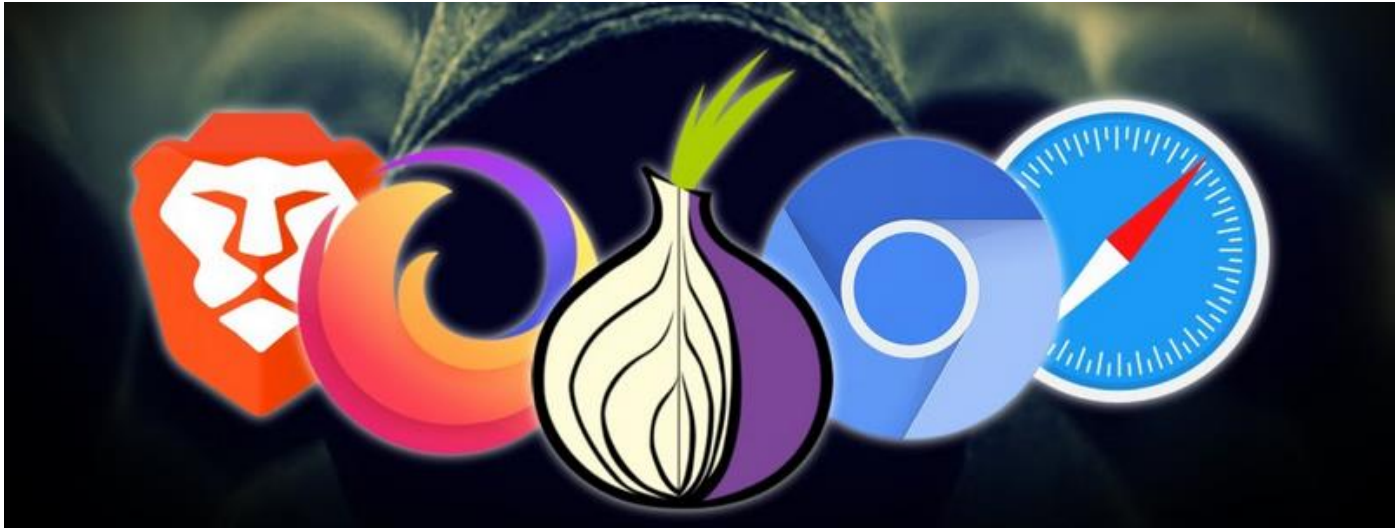
Whenever you sign into Google you'll enter your username and password as usual.

Enter code from phone*

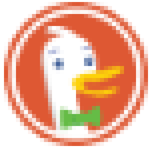
Next, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.

Afbeeldingsresultaat voor 2fa

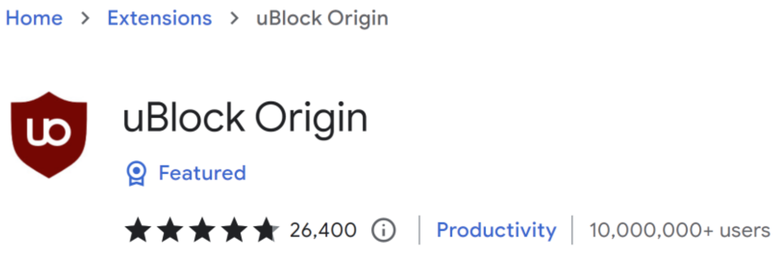
Install & use **ONLY these** web browsers!!!



Use **ONLY this** search engine



Install **these** web browser extensions **NOW**!!!

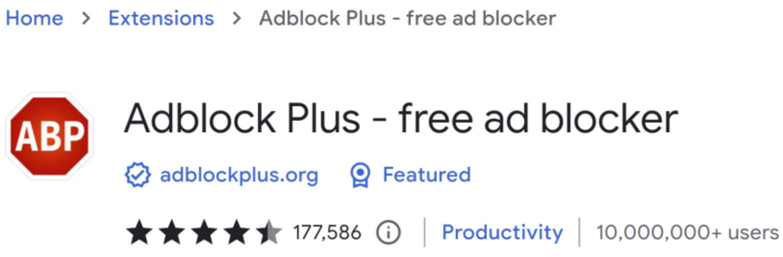


Home > Extensions > uBlock Origin

uBlock Origin

Featured

★★★★★ 26,400 ⓘ | Productivity | 10,000,000+ users

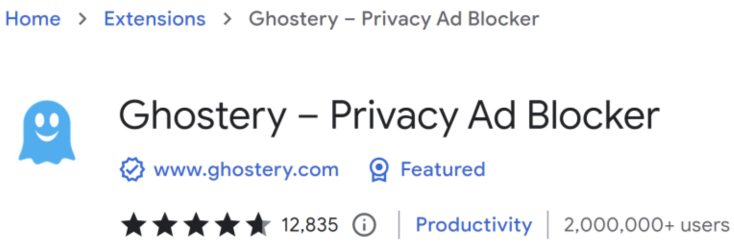


Home > Extensions > Adblock Plus - free ad blocker

Adblock Plus - free ad blocker

adblockplus.org Featured

★★★★★ 177,586 ⓘ | Productivity | 10,000,000+ users

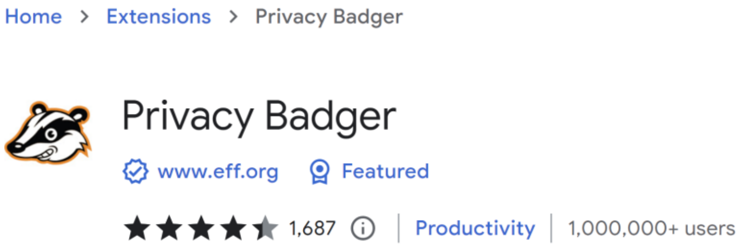


Home > Extensions > Ghostery – Privacy Ad Blocker

Ghostery – Privacy Ad Blocker

www.ghostery.com Featured

★★★★★ 12,835 ⓘ | Productivity | 2,000,000+ users



Home > Extensions > Privacy Badger

Privacy Badger

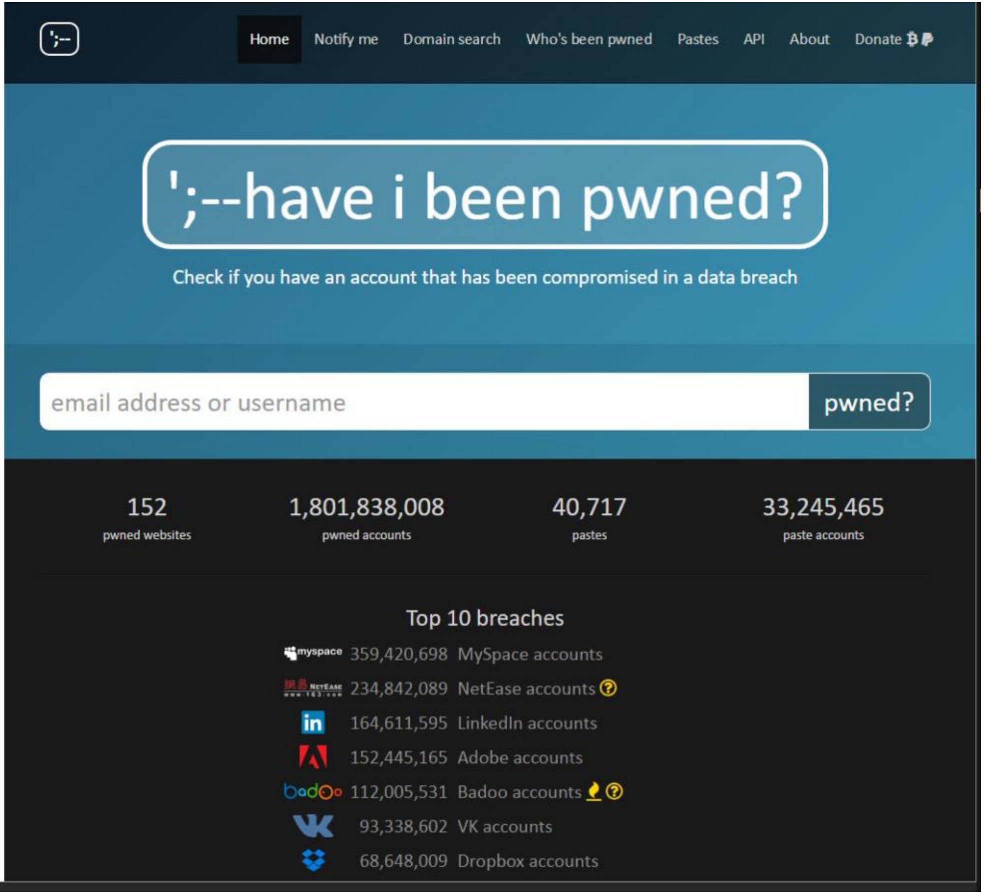
www.eff.org Featured

★★★★★ 1,687 ⓘ | Productivity | 1,000,000+ users

Data Breaches…

Are my password(s) known?

- Subscribe to: https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

152 pwned websites

1,801,838,008 pwned accounts

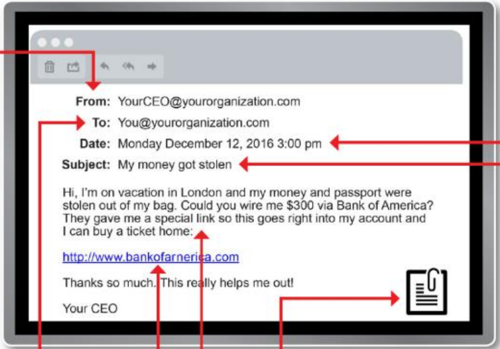
40,717 pastes

33,245,465 paste accounts

Top 10 breaches

359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
112,005,531	Badoo accounts
93,338,602	VK accounts
68,648,009	Dropbox accounts

Social Engineering Red Flags



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

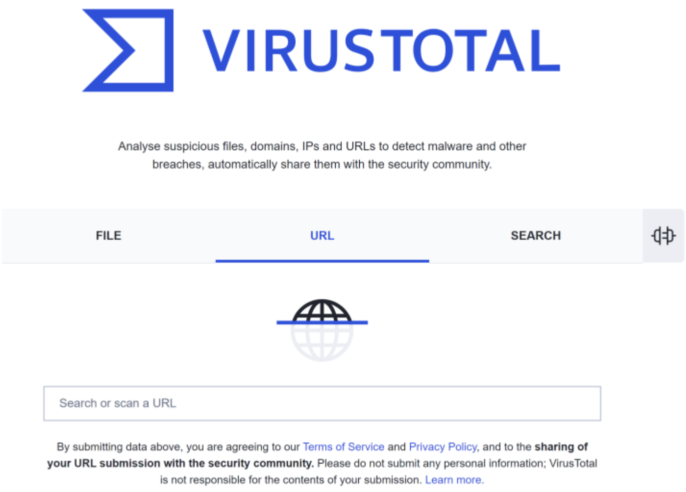
- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

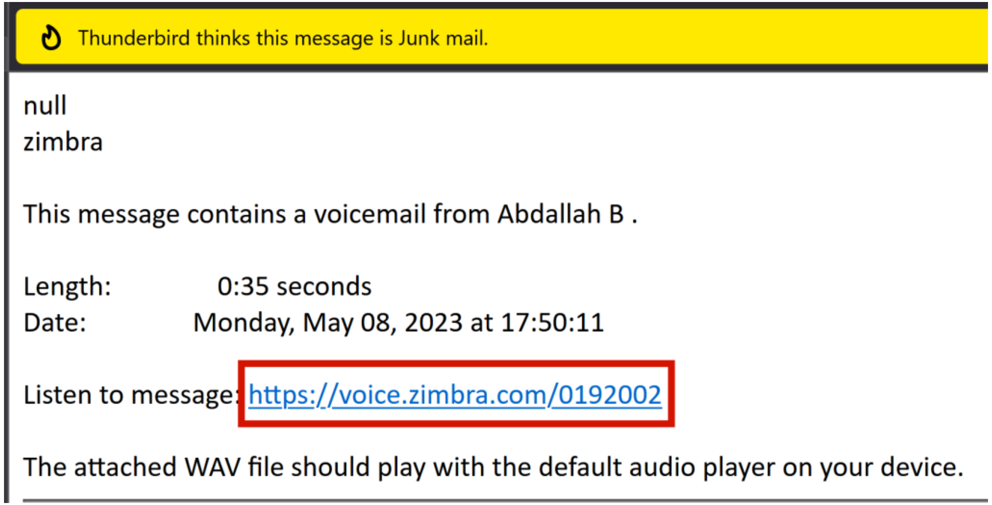
Data Breaches…



VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.



Thunderbird thinks this message is Junk mail.

null
zimbra

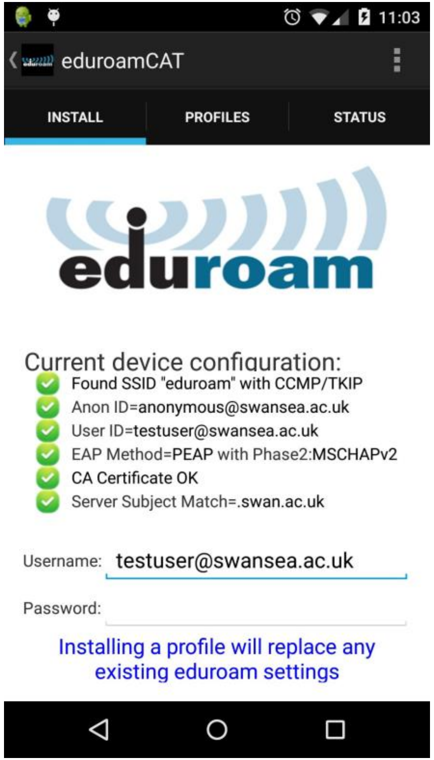
This message contains a voicemail from Abdallah B .

Length: 0:35 seconds
Date: Monday, May 08, 2023 at 17:50:11

Listen to message: https://voice.zimbra.com/0192002

The attached WAV file should play with the default audio player on your device.

eduroam CAT and geteduroam

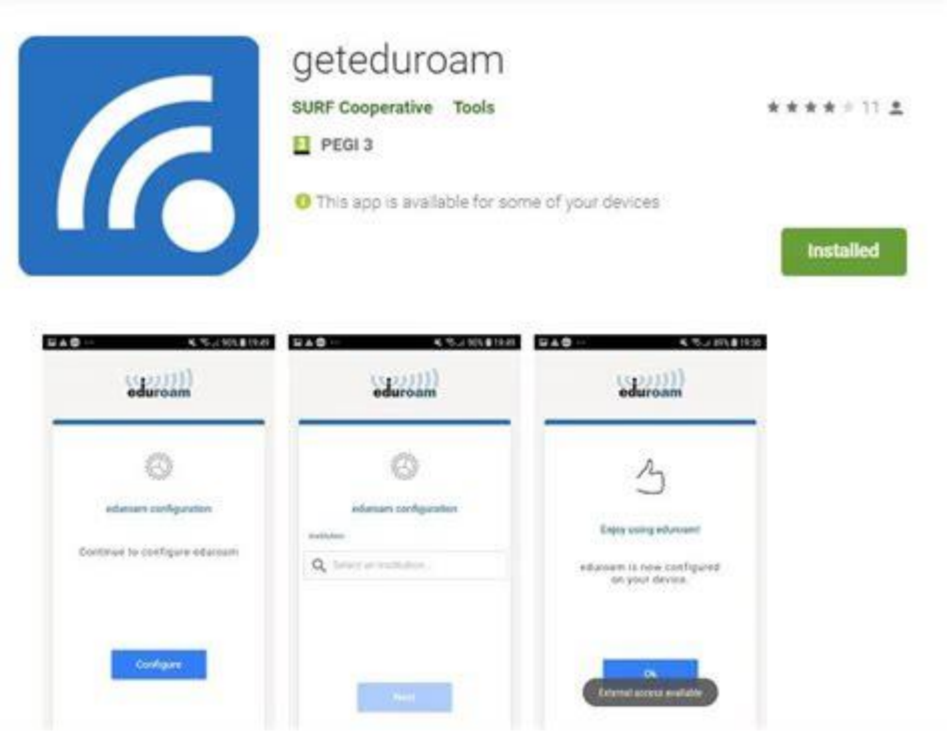


Current device configuration:
- ✓ Found SSID "eduroam" with CCMP/TKIP
- ✓ Anon ID=anonymous@swansea.ac.uk
- ✓ User ID=testuser@swansea.ac.uk
- ✓ EAP Method=PEAP with Phase2:MSCHAPv2
- ✓ CA Certificate OK
- ✓ Server Subject Match=.swan.ac.uk

Username: testuser@swansea.ac.uk

Password:

Installing a profile will replace any existing eduroam settings



This app is available for some of your devices

eduroam configuration

Continue to configure eduroam

eduroam configuration

Institution

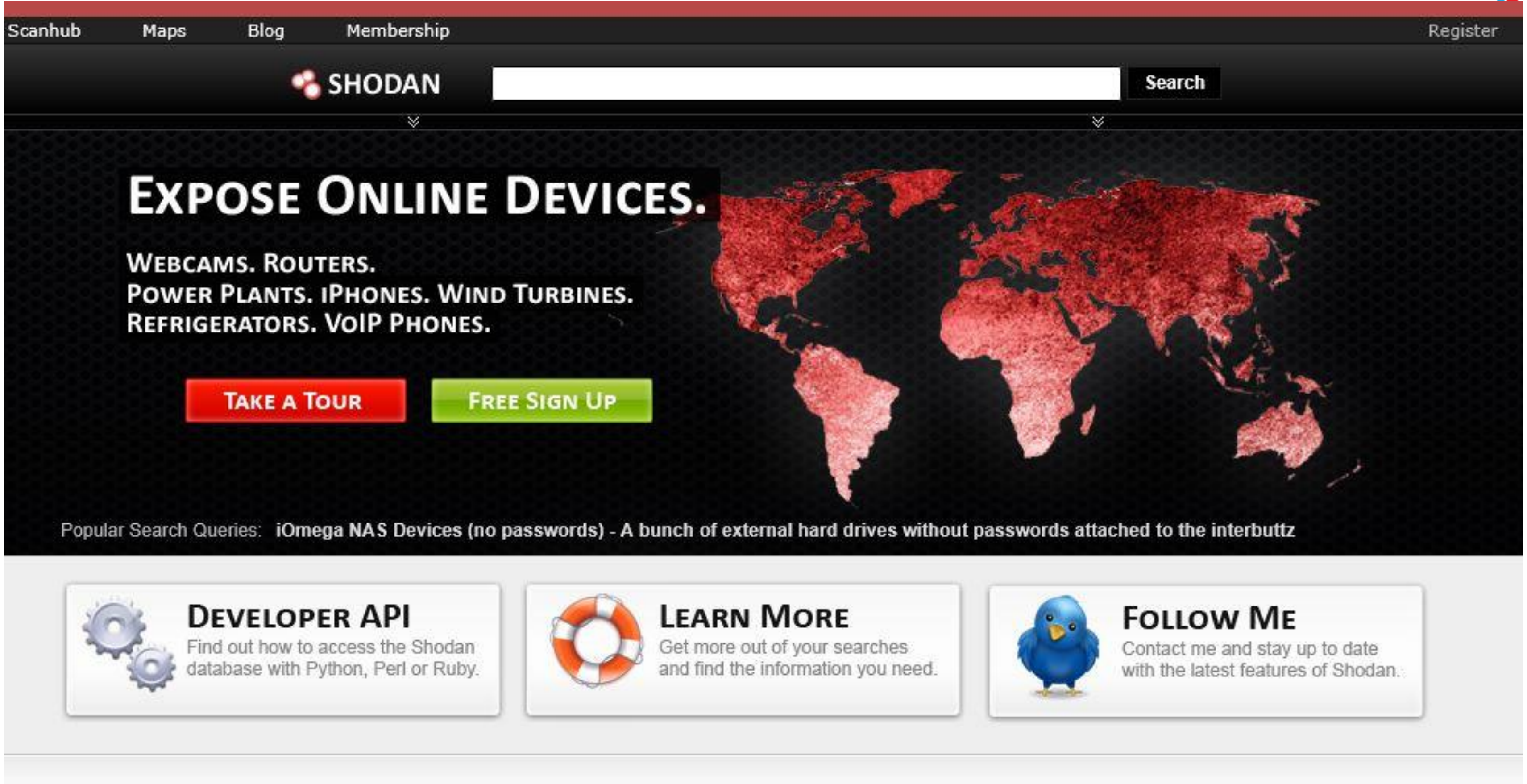
Select an institution...

Enjoy using eduroam!

eduroam is now configured on your device.

External access available

Data Breaches…



Scanhub Maps Blog Membership Register

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

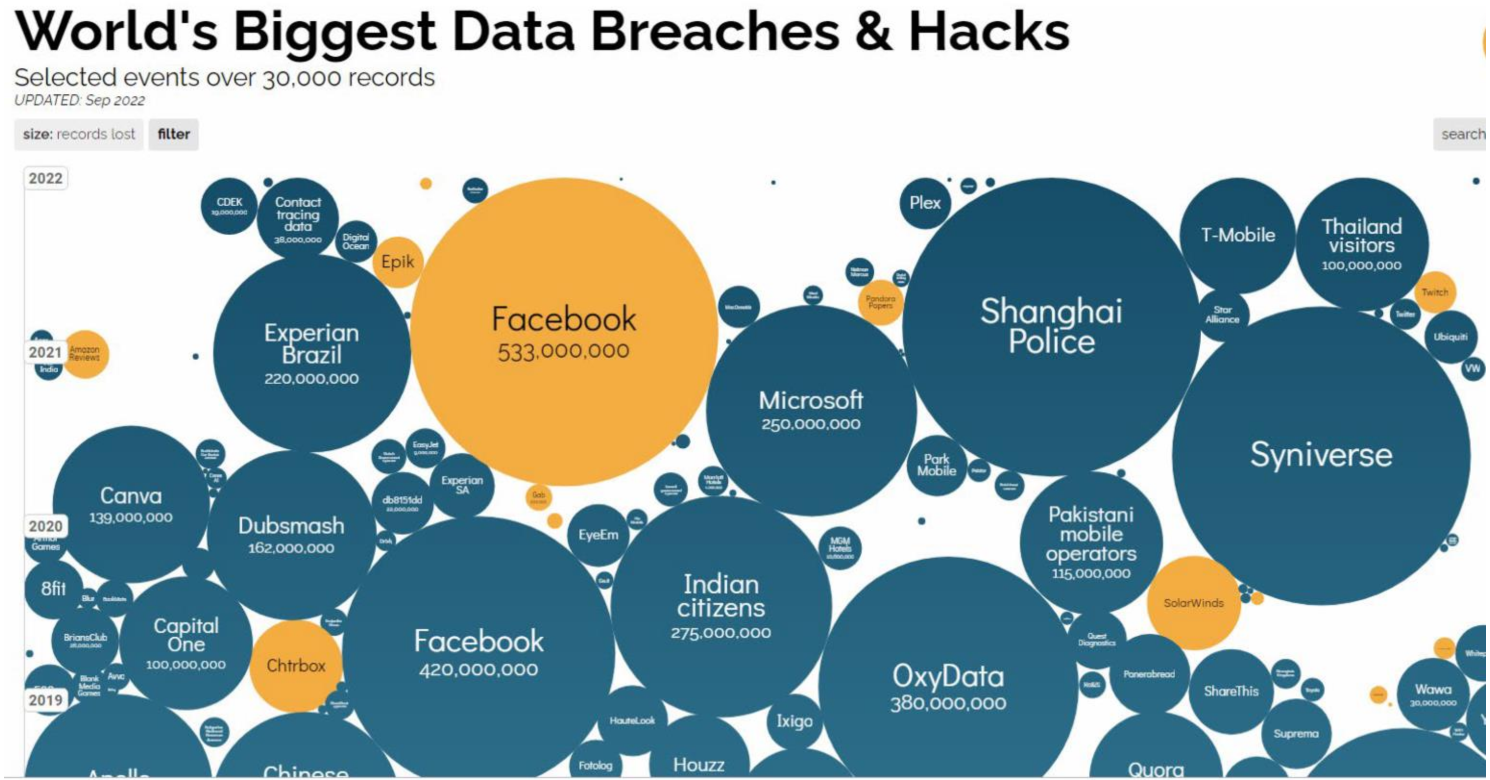
Popular Search Queries: iOmega NAS Devices (no passwords) - A bunch of external hard drives without passwords attached to the interbuttz

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

Data Breaches…



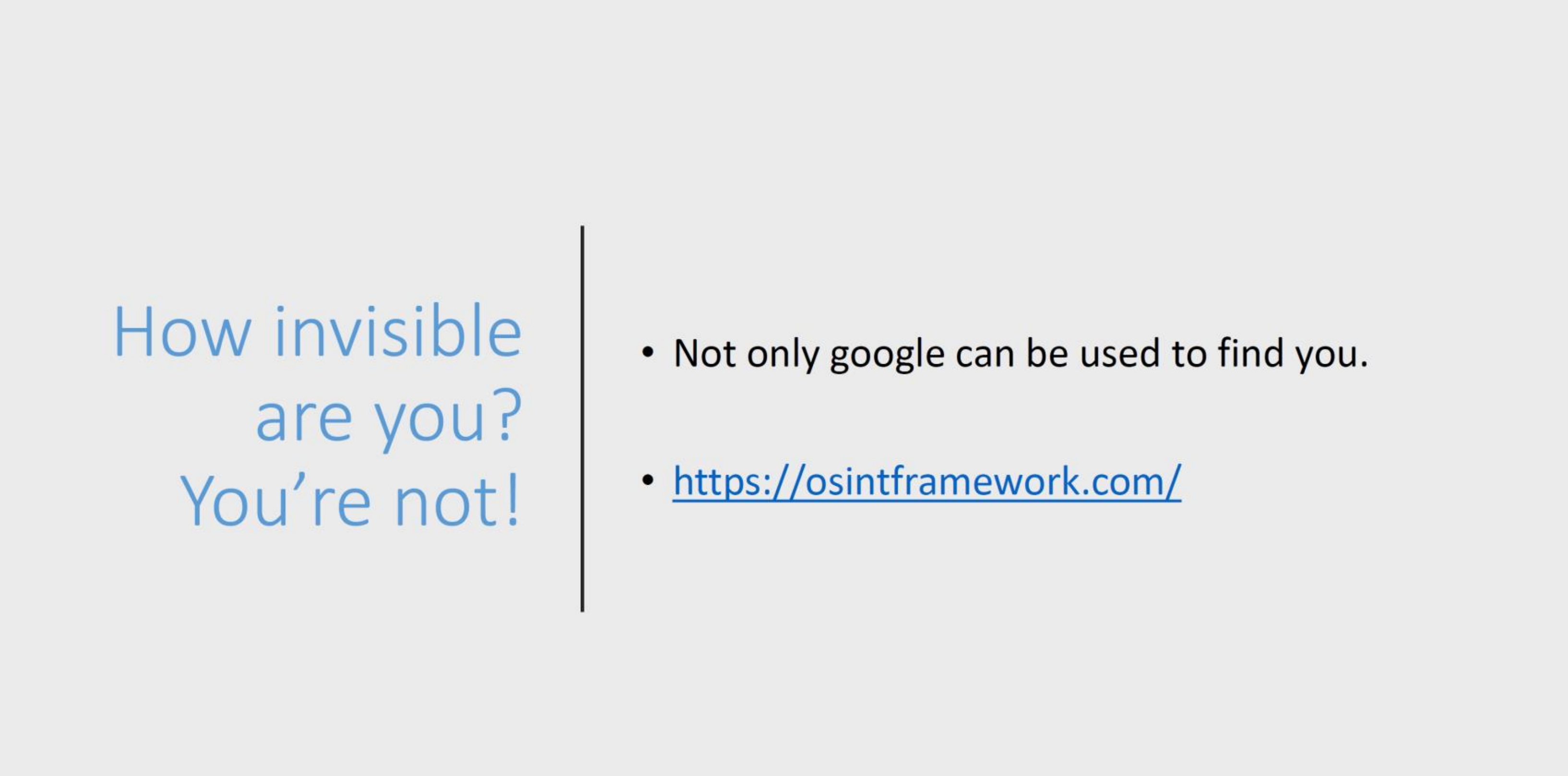
World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

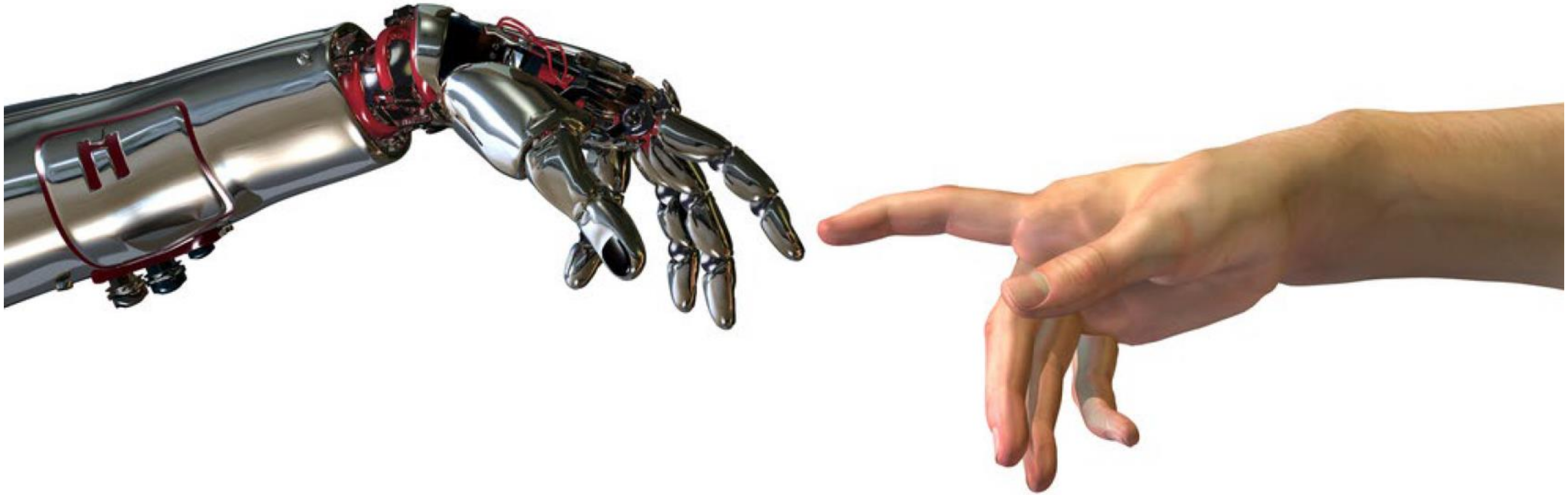
Data Breaches…

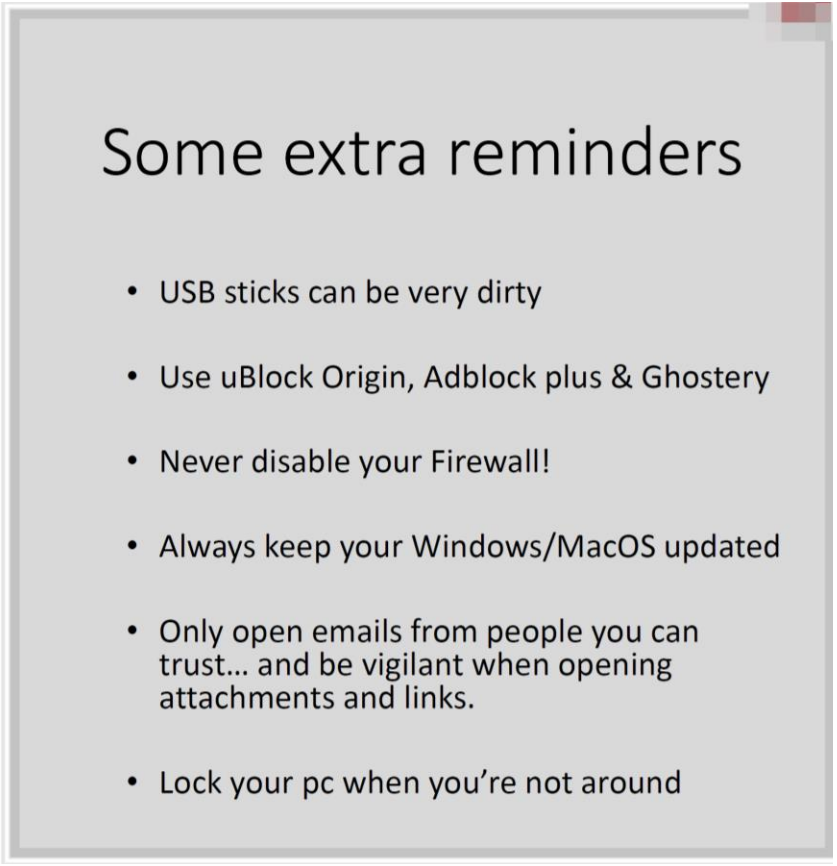


How invisible are you? You're not!

- Not only google can be used to find you.
- https://osintframework.com/

Security is technology <u>and people</u>




Some extra reminders

- USB sticks can be very dirty
- Use uBlock Origin, Adblock plus & Ghostery
- Never disable your Firewall!
- Always keep your Windows/MacOS updated
- Only open emails from people you can trust… and be vigilant when opening attachments and links.
- Lock your pc when you’re not around

QnA + Discussion

Write to cert@renu.ac.ug
For anything cybersecurity-related

SECURITY IS **EVERYONE'S** RESPONSIBILITY